

Pure Storage Integration with the F5 Privileged User Access Solution

2019 F5 Government Solutions

Pre-requisites

- Working and tested F5 Privileged User Access Solution
- IP Address of Pure Storage Management Interface(s)
- A working LDAP or Active Directory infrastructure, with Pure Storage pre-requisites for authorization (see notes)
- Pure Storage configured for Directory Authentication (below)

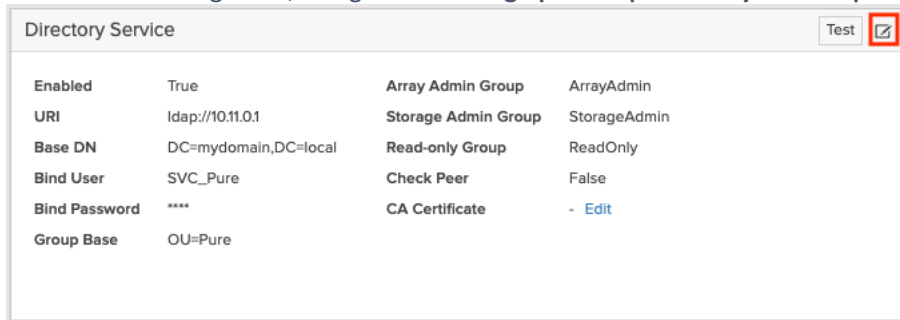
Pure Storage Configuration

Overview

This requires a directory service configuration is completed on the Pure Storage cluster/server.

Configuration

1. On the Pure Storage unit, navigate to **Settings | Users | Directory Service | Edit** (pencil box icon)

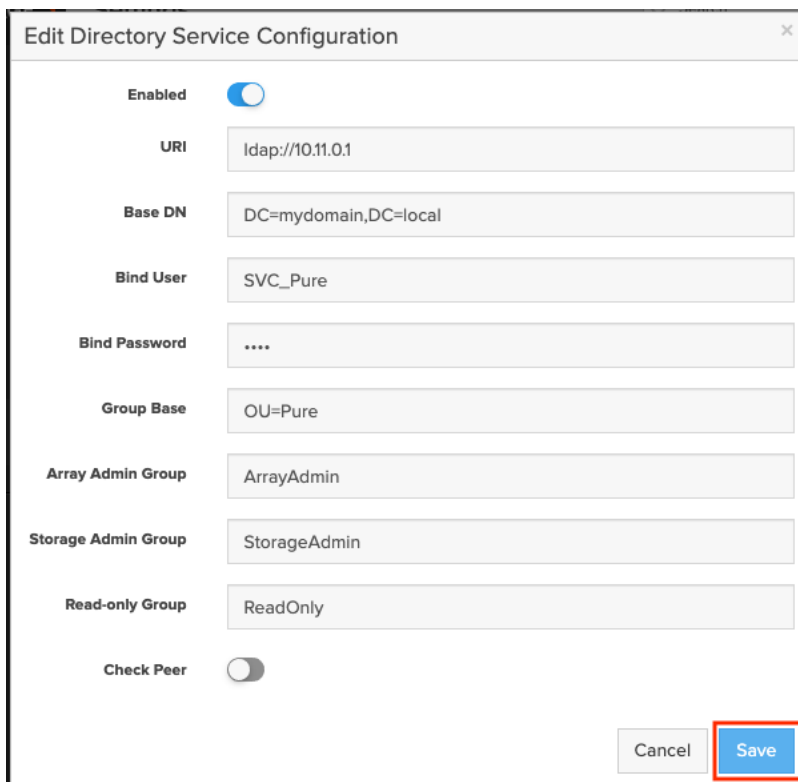


Directory Service

Enabled	True	Array Admin Group	ArrayAdmin
URI	ldap://10.11.0.1	Storage Admin Group	StorageAdmin
Base DN	DC=mydomain,DC=local	Read-only Group	ReadOnly
Bind User	SVC_Pure	Check Peer	False
Bind Password	****	CA Certificate	- Edit
Group Base	OU=Pure		

2. Fill out the required fields. An example is shown below and click **Save**

NOTE: the URI should be the LDAP(S) Proxy VIP on the BIG-IP and not the real LDAP/AD server. You may use the real LDAP/AD server initially for testing, then test with the BIG-IP LDAP Proxy VIP.

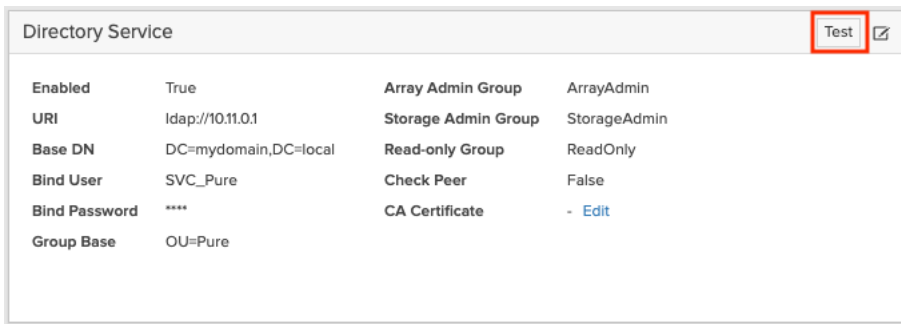


Edit Directory Service Configuration

Enabled	<input checked="" type="checkbox"/>
URI	ldap://10.11.0.1
Base DN	DC=mydomain,DC=local
Bind User	SVC_Pure
Bind Password	****
Group Base	OU=Pure
Array Admin Group	ArrayAdmin
Storage Admin Group	StorageAdmin
Read-only Group	ReadOnly
Check Peer	<input type="checkbox"/>

Cancel Save

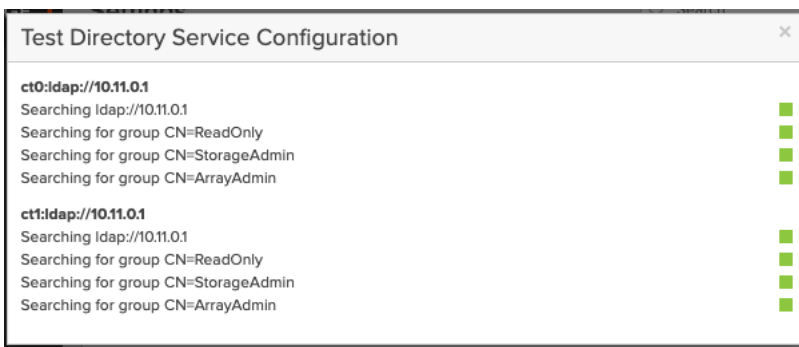
3. Click the **Test** button



Directory Service

Enabled	True	Array Admin Group	ArrayAdmin
URI	ldap://10.11.0.1	Storage Admin Group	StorageAdmin
Base DN	DC=mydomain,DC=local	Read-only Group	ReadOnly
Bind User	SVC_Pure	Check Peer	False
Bind Password	****	CA Certificate	- Edit
Group Base	OU=Pure		

4. You should see all green. If you do not, go no further until this issue is resolved. Refer to Pure Storage support for proper configuration. This test may also be done against the actual LDAP / AD server instead of the F5 VIP initially to ensure everything is configured correctly on the directory side.



Test Directory Service Configuration

ct0:ldap://10.11.0.1	
Searching ldap://10.11.0.1	■
Searching for group CN=ReadOnly	■
Searching for group CN=StorageAdmin	■
Searching for group CN=ArrayAdmin	■
ct1:ldap://10.11.0.1	
Searching ldap://10.11.0.1	■
Searching for group CN=ReadOnly	■
Searching for group CN=StorageAdmin	■
Searching for group CN=ArrayAdmin	■

Notes

Pure Storage Directory Requirements

Pure storage requires the following for LDAP/AD Authentication and Authorization

The FlashArray requires three access roles:

- **Array Admin Group:** Administrators that are allowed to perform every FlashArray operation including configuration—Array Admin Group administrators have the same privileges as the original built-in pureuser.
- **Storage Admin Group:** Administrators that are allowed to perform FlashArray storage operations (provision, snap etc).
- **Read Only Group:** Users with read-only privileges on the FlashArray—they can view information but not provision/change anything.

These role groups MUST reside in an OU

BIG-IP Configuration

Overview

SSO to the Pure Storage GUI requires injection of custom JavaScript to the login page. This is accomplished by using an internal VIP for the APM portal resource and assigning an iRule to inject the JavaScript on that VIP. This VIP will be restricted to the APM connectivity profile VLAN and the IP address is arbitrary but should not be overlapping.

LTM Configuration

1. Navigate to **LTM | Virtual Servers | Create**
2. **Name:** purestorage_cluster_proxy
3. **Type:** standard
4. **Destination Address/Mask:** <available IP, may be non-routable>
5. **Service Port:** available port <if creating multiple, reuse the IP address above with different ports>
6. **HTTP profile:** http

General Properties	
Name	PureStorage_cluster_proxy
Description	
Type	Standard
Source Address	
Destination Address/Mask	192.168.255.209
Service Port	9443 Other:
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Basic	
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile	http

7. **SSL Profile (client):** clientssl
8. **SSL Profile (server):** serverssl

	Selected	Available
SSL Profile (Client)	/Common clientssl	/Common auto_billchurch.me clientssl-insecure-compatible clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	/Common serverssl	/Common apm-default-serverssl crypto-client-default-serverssl pcolp-default-serverssl serverssl-insecure-compatible

9. **VLAN and Tunnel Traffic:** enabled on... <APM connectivity VLAN profile>
10. **Source Address Translation:** Auto Map

VLAN and Tunnel Traffic	Enabled on...				
VLANs and Tunnels	<table><thead><tr><th>Selected</th><th>Available</th></tr></thead><tbody><tr><td>/Common pua-connectivity</td><td>/Common VLAN_10 VLAN_20 VLAN_99 http-tunnel</td></tr></tbody></table>	Selected	Available	/Common pua-connectivity	/Common VLAN_10 VLAN_20 VLAN_99 http-tunnel
Selected	Available				
/Common pua-connectivity	/Common VLAN_10 VLAN_20 VLAN_99 http-tunnel				
Source Address Translation	Auto Map				

11. iRules: PureStorage-SSO-fix.tcl

12. Default Pool: <new>

- a. **Name:** purestorage_cluster_pool
- b. **Node Name:** purestorage_cluster
- c. **Address:** 192.168.20.20
- d. **Service Port:** 8443
- e. **Add**
- f. **Finished**

13. Click **Finished**

APM Pure Storage Web GUI Configuration

1. Navigate to **Access | Connectivity / VPN | Portal Access | Create**
 - a. **Name:** PureStorage_cluster
 - b. **Patching:** Full Patching
 - i. HTML Patching
 - ii. JavaScript Patching
 - iii. CSS Patching

- iv. Flash Patching
- c. **Publish on Webtop:** Enable
- d. **Link Type:** Application URI
- e. **Application URI:** https://<ip in step 4 of LTM configuration>
- f. **Caption:** Pure Storage Cluster
- g. **Image:** <any desired image for customization, or leave default>
- h. Click **Create**

Access » Connectivity / VPN : Portal Access : Portal Access Lists » **New Resource...**

General Properties

Name	PureStorage_cluster
Description	
ACL Order	Last

Configuration: Basic

Match Case For Paths	Yes
Patching	Type: Full Patching <input checked="" type="checkbox"/> HTML Patching <input checked="" type="checkbox"/> JavaScript Patching <input checked="" type="checkbox"/> CSS Patching <input checked="" type="checkbox"/> Flash Patching <input type="checkbox"/> Java Patching
Publish on Webtop	<input checked="" type="checkbox"/> Enable
Link Type	Application URI
Application URI	https://192.168.255.209:9443

Customization Settings for English

Language	English
Caption	Pure Storage Cluster
Detailed Description	
Image	Choose File purestoragelogo View/Hide

Cancel Create

2. Under **Resource Items** click **Add**
 - a. **Link Type:** Paths
 - b. **Destination:** IP Address <IP of purestorage_cluster_proxy>
 - c. **Paths:** /*
 - d. **Scheme:** https
 - e. **Port:** <port of purestorage_cluster_proxy>
 - f. **Compression:** GZIP Compression
 - g. **Client Cache:** No Cache
 - h. **SSO Configuration:** None
 - i. Click **Finished**

Access » Connectivity / VPN : Portal Access : Portal Access Lists » PureStorage_cluster

New Resource Item...: Advanced ▾

Link Type	Paths ▾
Destination	Type: <input type="radio"/> Host Name <input checked="" type="radio"/> IP Address IP Address 192.168.255.209
Paths	/*
Scheme	https ▾
Port	9443
Headers	Name <input type="text"/> Value <input type="text"/> Add <input type="text"/> Edit Delete

Resource Item Properties: Basic ▾

Compression	GZIP Compression ▾
Client Cache	No Cache ▾
SSO Configuration	None ▾
Log	None ▾

Cancel Finished

3. Navigate to **Access | Profiles / Policies : Access Profiles (Per-Session Policies)**
 - a. Click **Edit** next to the desired PUA policy
 - b. Click the resource assignment (Advanced Resource Assign, LDAP Group Resource Assign, etc...)

- c. Add the newly created portal resource to the desired group or branch and save.

Properties | **Branch Rules**

Name: LDAP Group Resource Assign

LDAP Group Resource Assign

Server: /Common/ad_server

Begin typing to search

Add new entry Insert Before: 1

Groups	Portal Access	Remote Desktop	Webtop Links	Webtop	Webtop Sections
1 Lab Managers	PureStorage_cluster sample_pua_policy-webssh_portal	DC1		Lab_Managers	No_Demo
2 RouterEnable RouterView	BIGIP Fidelis Palo_Alto_Web sample_pua_policy-webssh_portal		BIG-IP GenCred Palo_Alto_SSH PureStorage_SSH Solaris_10 SSH_Host_1 SSH_Host_2	sample_pua_policy	BIG-IP Firewall Linux_Hosts No_Demo No_SSO Solaris Storage
3 Storage Managers	BIGIP PureStorage sample_pua_policy-webssh_portal		BIG-IP PureStorage_SSH	sample_pua_policy	Storage

Cancel Save Help

- d. Apply the policy

APM WebSSH Client Configuration

1. Navigate to **Access | Webtops | Webtop Links** and click **Create**
2. Create a new webtop link to the existing WebSSH2 portal resource, using the actual IP address of the Pure Storage Cluster SSH service

Access >> Webtops : Webtop Links >> PureStorage_SSH

⚙️ Properties

General Properties

Name	PureStorage_SSH
Partition / Path	Common
Description	

Configuration

Link Type	Application URI
Application URI	https://%(session.server.network.name)/f5-w-68747470733a2f2f3139322e3

Customization Settings for English

Language	English
Caption	PureStorage SSH
Detailed Description	Remote Tunnel - Reston
Image	Choose File No file chosen View/Hide

Update Delete

3. Add this new webtop link to the APM policy as described previously

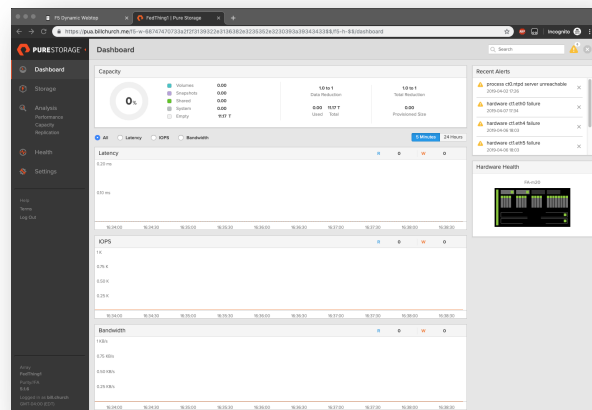
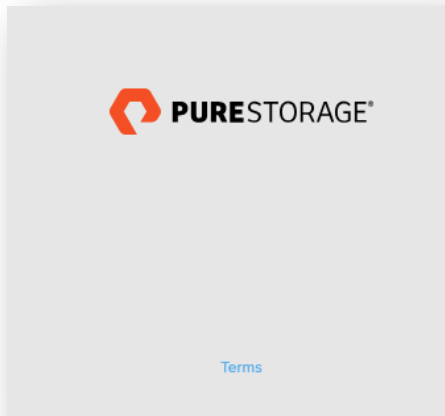
Validation

Using a client, browse to the PUA Webtop interface and attempt to log into the newly created Pure Storage GUI resource...

 Other Resources

 Pure Storage Cluster

During the SSO event, you may see the form field flash and disappear, or it may appear as below. This is normal.



After a few moments, the Pure Storage Dashboard should appear:

Now do the same for the SSH resource

 PureStorage SSH
Remote Tunnel - Reston

